Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Dec 13 - 19, 2022

Report Summary:

- **New Threat Detection Added** – 06 (GootLoader Malware, DolphinCape Malware, PyPi-NPM CIA Ransomware, BlackMagic Ransomware, CHAOS RAT and DEV-1028 botnet)
- **New Threat Protections**
- **Overall Weekly Observables Count**
- **Daily submissions by Observable Type**
- **New Ransomware Victims Last Week**

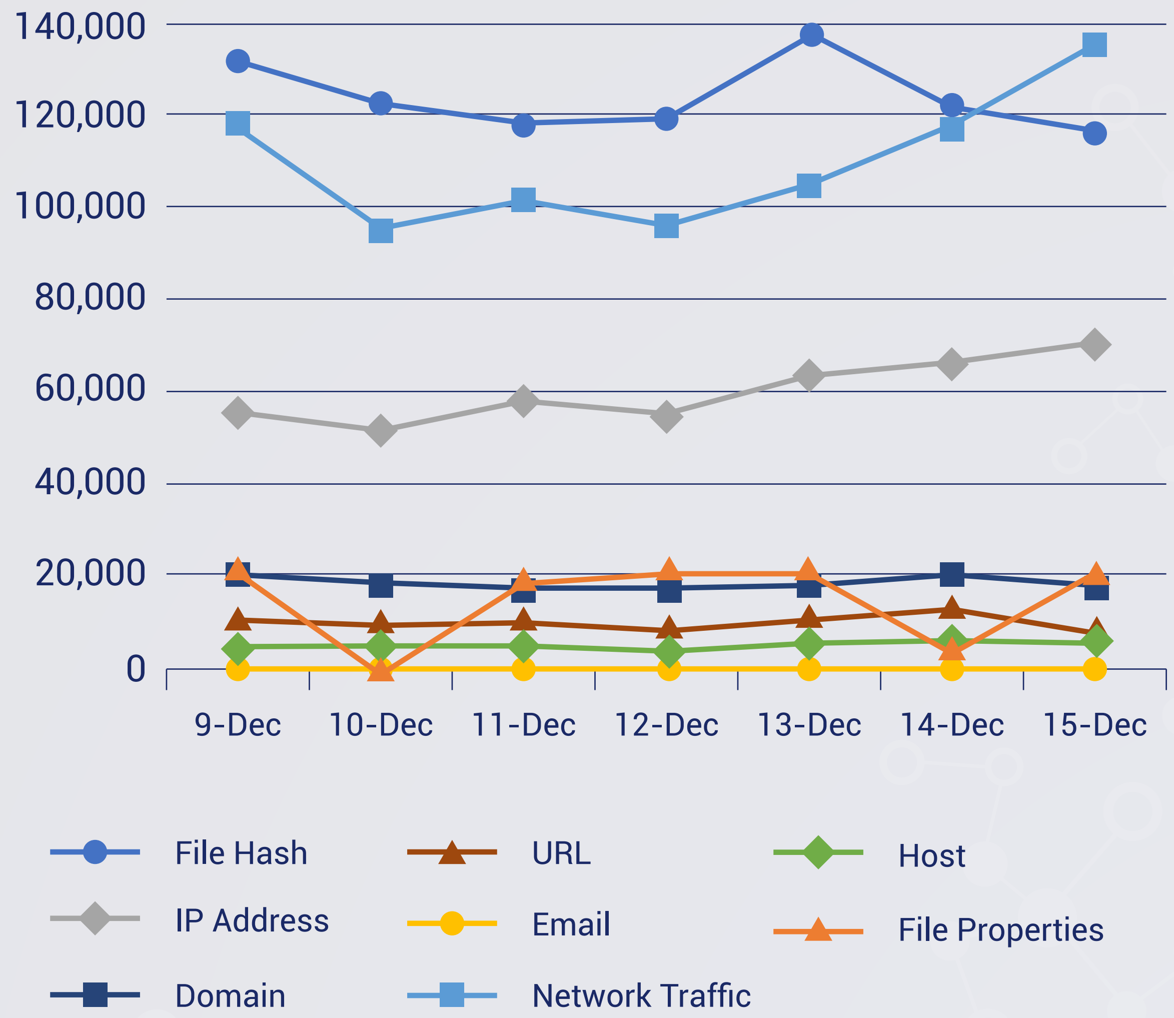
New Threat Protections (Week Ending 19/12/2022):

9

Overall Weekly Observables Count:

2,331,551

Daily Submissions by Observable Type:



Newly Detected Threats Added

1. GootLoader Malware

Gootloader aka Gootkit was originally delivered through spam campaigns and legacy exploit kits. Gootloader operators are increasingly observed using search engine optimization (SEO) poisoning tactics to gain access to victims' environments and initiate multifaceted breaches involving subsequent payloads such as Cobalt Strike and Gootkit. Gootloader poses a significant threat to enterprise environments because it is designed to deliver additional malware. Gootloader operators compromise legitimate infrastructures like WordPress blogs and seed these sites with common keywords. The operators then use SEO techniques to direct anyone who types these keywords into a search engine to a page that entices the user to download a ZIP file containing the initial Gootloader script. Most observed Gootloader campaigns involved initial malicious ZIP files containing the word "contract" in the file name.

Threat Protected: 01
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

Class Type: Trojan-activity
Kill Chain: Persistence T1574.002 - Privilege Escalation T1055/T1574.002 - Defense Evasion T1055/T1218.010/T1218.011 - Discovery T1082 - Command and Control T1071

2. DolphinCape Malware

According to the latest CERT-UA advisory, the new malicious campaign against the state railway transport organization of Ukraine "Ukrzaliznytsia" used a phishing email delivering DolphinCape malware developed with Delphi to targeted users. In this attack, threat actors send out decoy emails that promise to reveal information on how to identify Iran's Shahed-136 drones. The infection chain starts by opening a decoy RAR file attachment that contains a PPSX document with malicious VBScript code. It is designed to generate a scheduled task and decrypt, create, and run a PowerShell script. The hackers use the RC4 encryption algorithm, and a key created by concatenating the value string of the "Manager" attribute and the file name. The malicious PowerShell script will use the BITS component of Microsoft Windows to download DLL and EXE files and create a scheduled task to run the latter using the DLL sideloading technique. The DLL file is identified as DolphinCape malware, which collects information about hostname, username, and operating system version, and exfiltrates other data from infected computers executes EXE and DLL files and displays a list of files and their uploads. DolphinCape malware is also capable of capturing screenshots from target computers.

Threat Protected: 01
Rule Set Type:

Class Type: Trojan- Activity
Kill Chain: Initial Access T1566 - Defense Evasion T1218/T1216/T1197 - Execution T1059/T1053

Ruleset	IDS: Action	IPS: Action
Balanced	Alert	Alert
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

3. PyPi-NPM CIA Ransomware

An ongoing distribution of a CIA-themed ransomware that targets PyPi users has been discovered. Python's 'requests' package has been a target of typosquatting. The threat actor published ransomware binaries written in Golang disguised as a legitimate Python package. It was determined that NPM packages are also being affected. Upon execution of malware, it will immediately change the background screen with a fake message from the CIA and will start encrypting the victim's files.

Threat Protected: 02
Rule Set Type:

Class Type: Trojan- Activity
Kill Chain: Initial Access T1189/T1566 - Execution T1106 - Impact T1486

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

4. BlackMagic Ransomware

A ransomware that targets the logistics sector. The threat group exfiltrates their victims' data first and then encrypts it. Their ransom notes do not contain any links to where they can be paid, instead, they contain links to where the data is dumped and sold. Upon execution, the malware kills system processes, disables the task manager via registry, gathers information from the system then sends a request to its remote Command-and-Control server. After encryption, it creates a batch file that cleans up its traces and changes the screen background.

Threat Protected: 01
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Alert	Alert
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

Class Type: Trojan-activity
Kill Chain: Execution T1059 - Defense Evasion T1218 - Command-and-Control T1071 - Impact T1486

5. CHAOS RAT

A cryptocurrency mining attack targeting the Linux operating system has recently included the use of an open-source remote access trojan known as CHAOS. The RAT alters /etc/crontab file, a UNIX task scheduler that downloads itself every 10 minutes from Pastebin to achieve persistence. Once downloaded and launched, it transmits system metadata to a remote server. It is GO Compiled with capabilities to carry out the following operations.

- Perform reverse shell
- Download files
- Upload files
- Delete files
- Take screenshots
- Access file explorer
- Gather operating system information
- Restart the PC
- Shutdown the PC
- Open a URL

Threat Protected: 02
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

Class Type: Trojan-activity
Kill Chain: Initial Access T1566/T1189 - Execution T1106/T1059 - Command-and-Control T1102

6. DEV-1028 botnet

A new cross-platform botnet has been found originating from malicious software downloads on Windows devices and succeeds in infecting Linux-based devices like Minecraft servers. The botnet spreads by enumerating default credentials on internet-exposed Secure Shell (SSH)-enabled devices. IoT devices with remote configuration enabled and configured with potentially insecure settings are at risk to attacks like this botnet. The botnet's spreading mechanism makes it uniquely interesting. While the malware can be removed from the infected source PC, it could persist on unmanaged IoT devices in the network and continue to operate as part of the botnet.

Threat Protected: 02
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Alert	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Disabled	Disabled

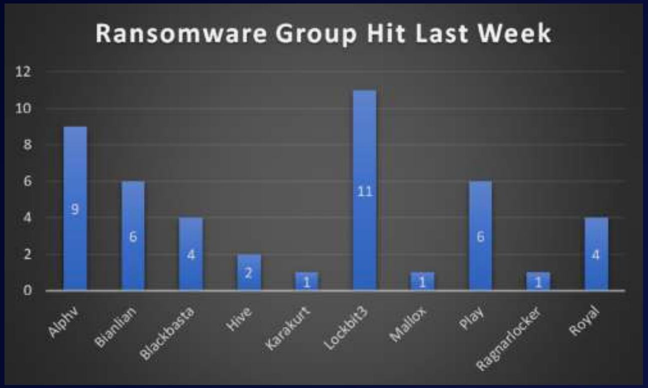
Class Type: Malware
Kill Chain: Execution TA0002 - Persistence TA0003 - Privilege Escalation TA0004 - Defense Evasion TA0005 - Discovery TA0007 - Command and Control TA0011

New Ransomware Victims Last Week: 45

Red Piranha periodically collects information about organizations hit by ransomware from different sources including the Dark Web. During the previous week, Red Piranha identified a total of 45 new ransomware victim organizations.

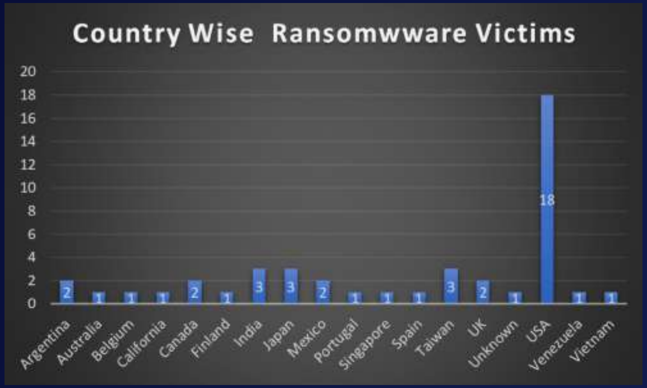
One particular group linked to the LockBit 3.0 ransomware tallied the greatest number of new victims (11), the locations of which are spread across different countries. This is followed by AlphaV and Bianlian groups with 9 and 6 new victims respectively. Victim counts these ransomware groups and a few others are listed below.

Alphv	-	9
Bianlian	-	6
Blackbasta	-	4
Hive	-	2
Karakurt	-	1
Lockbit3	-	11
Mallox	-	1
Play	-	6
Ragnarlocker	-	1
Royal	-	4



If we look at the victims as per the country, we can say that the USA was once again become the most targeted country by ransomware groups where a total of 18 new victims were reported last week followed by India and Japan where 3 new victims each were reported. The number of new ransomware victims per country is listed below:

Argentina	-	2	Portugal	-	1
Australia	-	1	Singapore	-	1
Belgium	-	1	Spain	-	1
California	-	1	Taiwan	-	3
Canada	-	2	UK	-	2
Finland	-	1	Unknown	-	1
India	-	3	USA	-	18
Japan	-	3	Venezuela	-	1
Mexico	-	2	Vietnam	-	1



Red Piranha Security Advisory – CVE-2022-37958

Red Piranha recently published an advisory on a newly discovered vulnerability in the SPNEGO, a protocol used between client and server applications (SMB, RDP, etc.) in a Windows environment to negotiate the authentication mechanisms to be used.

The vulnerability was assigned a high severity risk rating as it allows for a Remote-code Execution on successful exploitation.

Red Piranha advisory can be found in the link below:

https://redpiranha.net/news/critical-remote-code-execution-spnego-cve-2022-37958-effects-windows-protocols-rdp-and-smb